EXHIBIT G

6.3 Implementation of risk control measure(s) (Step 6)

The manufacturer shall implement the risk control measure(s) selected in 6.2. The measure(s) used to control the risks shall be recorded in the risk management file.

The effectiveness of the risk control measures shall be verified and the results of the verification shall be recorded in the risk management file.

Implementation of the risk control measures shall be verified. This verification shall also be recorded in the risk management file.

Compliance is checked by inspection of the risk management file.

6.4 Residual risk evaluation (Step 7)

Any residual risk that remains after the risk control measure(s) are applied shall be evaluated using the criteria defined in the risk management plan. The results of this evaluation shall be recorded in the risk management file.

If the residual risk does not meet these criteria, further risk control measures shall be applied (see 6.2).

If the residual risk is judged acceptable, then all relevant information necessary to explain the residual risk(s) shall be placed in the appropriate accompanying documents supplied by the manufacturer.

Compliance is checked by inspection of the risk management file and the accompanying documents.

6.5 Risk/benefit analysis (Step 8)

If the residual risk is judged unacceptable using the criteria established in the risk management plan and further risk control is impractical, the manufacturer shall gather and review data and literature on the medical benefits of the intended use/intended purpose to determine if they outweigh the residual risk. If this evidence does not support the conclusion that the medical benefits outweigh the residual risk, then the risk remains unacceptable. If the medical benefits outweigh the residual risk, then proceed to 6.6. Relevant information necessary to explain the residual risk shall be placed in the appropriate accompanying documents supplied by the manufacturer. The results of this evaluation shall be recorded in the risk management file.

Compliance is checked by inspection of the risk management file and the accompanying documents.

6.6 Other generated hazards (Step 9)

The risk control measures shall be reviewed to identify if other hazards are introduced. If any new hazards are introduced by any risk control measures, the associated risk(s) shall be assessed (see 4.4). The results of this review shall be recorded in the risk management file.

Compliance is checked by inspection of the risk management file.

6.7 Completeness of risk evaluation (Step 10)

The manufacturer shall assure that the risk(s) from all identified hazards have been evaluated. The results of this assessment shall be recorded in the risk management file.

Compliance is checked by inspection of the risk management file.

7 Overall residual risk evaluation (Step 11)

After all risk control measures have been implemented and verified, the manufacturer shall decide if the overall residual risk posed by the medical device is acceptable using the criteria defined in the risk management plan. If the overall residual risk is judged unacceptable using the criteria established in the risk management plan, the manufacturer shall gather and review data and literature on the medical benefits of the intended use/intended purpose to determine if they outweigh the overall residual risk. If this evidence does not support the conclusion that the medical benefits outweigh the overall residual risk, then the risk remains unacceptable. The results of the overall residual risk evaluation shall be recorded in the risk management file.

Compliance is checked by inspection of the risk management file.

8 Risk management report (Step 12)

The results of the risk management process shall be recorded in a risk management report. The risk management report shall provide traceability for each hazard to the risk analysis, the risk evaluation, the implementation and

verification of the risk control measures, and the assessment that the residual risk(s) is acceptable. The risk management report shall form part of the risk management file.

NOTE—This report may be held on paper or on electronic media.

Compliance is checked by inspection of the risk management report.

9 Post-production information (Step 13)

The manufacturer shall establish and maintain a systematic procedure to review information gained about the medical device or similar devices in the post-production phase. The information shall be evaluated for possible relevance to safety, especially the following:

a) if previously unrecognized hazards are present;

b) if the estimated risk(s) arising from a hazard is no longer acceptable;

c) if the original assessment is otherwise invalidated.

If any of the above conditions is satisfied, the results of the evaluation shall be fed back as an input to the risk management process (see 4.4).

In the light of this safety relevant information, a review of the appropriate steps of risk management process for the medical device shall be considered. If there is a potential that the residual risk(s) or its acceptability has changed, the impact on previously implemented risk control measures shall be evaluated.

The results of this evaluation shall be recorded in the risk management file.

NOTE 1—Some aspects of post-production monitoring are the subject of national or regional regulations. In some cases, additional measures, e.g., prospective post-production evaluations, might be required.

NOTE 2—See also 4.14 of ISO 13485:1996.

NOTE 3—Information may be found at any stage of the medical device life cycle from inception to post-production phases.

Compliance is checked by inspection of the risk management process documentation and the risk management file.

Annex A
(informative)

Questions that can be used to identify medical device characteristics that could impact on safety

A.1 General

The first step in identifying hazards is to analyze the medical device for characteristics that could affect safety. One way of doing this is to ask a series of questions concerning the manufacture, use, and ultimate disposal of the medical device. If one asks these questions from the point of view of all the individuals involved (e.g., users, maintainers, patients, etc.), a more complete picture may emerge of where the potential hazards can be found. The following questions can aid the reader in identifying all the potential hazards of the medical device being analyzed.

The list is not exhaustive, and the reader is cautioned to add questions that may have applicability to the particular medical device.

A.2 Questions

A.2.1 What is the intended use/intended purpose and how is the medical device to be used?

Factors that should be considered include the intended user, the mental and physical abilities, skill, and training of the user, ergonomic aspects, the environment in which it is to be used, by whom it will be installed, and whether the patient can control or influence the use of the medical device. Special attention should be paid to intended users with special needs such as handicapped persons, the elderly, and children. Their special needs might include assistance by another person to enable the use of a medical device. Is the medical device intended to be used by individuals with various skill levels and cultural backgrounds?

What role is the medical device intended to play in the diagnosis, prevention, monitoring, treatment or alleviation of disease, compensation for injury or handicap, replacement or modification of anatomy, or control of conception? Is the medical device life sustaining or life supporting? Is special intervention necessary in the case of failure of the medical device? Are there special concerns about interface design features that could contribute to inadvertent use error (see A.2.27)?

A.2.2 Is the medical device intended to contact the patient or other persons?

Factors that should be considered include the nature of the intended contact, i.e., surface contact, invasive contact, and/or implantation and, for each, the period and frequency of contact.

A.2.3 What materials and/or components are incorporated in the medical device or are used with, or are in contact with, the medical device?

Factors that should be considered include whether characteristics relevant to safety are known.

A.2.4 Is energy delivered to and/or extracted from the patient?

Factors that should be considered include the type of energy transferred and its control, quality, quantity, and duration.

A.2.5 Are substances delivered to and/or extracted from the patient?

Factors that should be considered include whether the substance is delivered or extracted, whether it is a single substance or range of substances, the maximum and minimum transfer rates, and control thereof.

A.2.6 Are biological materials processed by the medical device for subsequent re-use?

Factors that should be considered include the type of process and substance(s) processed (e.g., auto-transfusion, dialysis).

A.2.7 Is the medical device supplied sterile or intended to be sterilized by the user, or are other microbiological controls applicable?

Factors that should be considered include whether the medical device is intended for single-use or to be re-usable, and also any packaging, the shelf-life, and any limitation on the number of re-use cycles or type of sterilization process to be used.

A.2.8 Is the medical device intended to be routinely cleaned and disinfected by the user?

Factors that should be considered include the types of cleaning or disinfecting agents to be used and any limitations on the number of cleaning cycles. In addition, the design of the medical device can influence the effectiveness of routine cleaning and disinfection.

A.2.9 Is the medical device intended to modify the patient environment?

Factors that should be considered include temperature, humidity, atmospheric gas composition, pressure, and light.

A.2.10 Are measurements taken?

Factors that should be considered include the variables measured and the accuracy and the precision of the measurement results.

A.2.11 Is the medical device interpretative?

Factors that should be considered include whether conclusions are presented by the medical device from input or acquired data, the algorithms used, and confidence limits.

A.2.12 Is the medical device intended for use in conjunction with medicines or other medical technologies?

Factors that should be considered include identifying any medicines or other medical technologies which can be involved and the potential problems associated with such interactions, as well as patient compliance with the therapy.

A.2.13 Are there unwanted outputs of energy or substances?

Energy-related factors that should be considered include noise and vibration, heat, radiation (including ionizing, non-ionizing, and ultraviolet/visible/infrared radiation), contact temperatures, leakage currents, and electric and/or magnetic fields.

Substance-related factors that should be considered include discharge of chemicals, waste products, and body fluids.

A.2.14 Is the medical device susceptible to environmental influences?

Factors that should be considered include the operational, transport, and storage environments. These include light, temperature, vibrations, spillage, susceptibility to variations in power and cooling supplies, and electromagnetic interference.

A.2.15 Does the medical device influence the environment?

Factors that should be considered include the effects on power and cooling supplies, emission of toxic materials, and the generation of electromagnetic interference.

A.2.16 Are there essential consumables or accessories associated with the medical device?

Factors that should be considered include specifications for such consumables or accessories and any restrictions placed upon users in their selection of these.

A.2.17 Is maintenance and/or calibration necessary?

Factors that should be considered include whether maintenance and/or calibration are to be carried out by the operator or user or by a specialist. Are special substances or equipment necessary for proper maintenance and/or calibration?

A.2.18 Does the medical device contain software?

Factors that should be considered include whether software is intended to be installed, verified, modified, or exchanged by the user and/or operator.

A.2.19 Does the medical device have a restricted shelf-life?

Factors that should be considered include labeling or indicators and the disposal of such medical devices.

A.2.20 Are there any delayed and/or long-term use effects?

Factors that should be considered include ergonomic and cumulative effects.

A.2.21 To what mechanical forces will the medical device be subjected?

Factors that should be considered include whether the forces to which the medical device will be subjected are under the control of the user or controlled by interaction with other persons.

A.2.22 What determines the lifetime of the medical device?

Factors that should be considered include aging and battery depletion.

A.2.23 Is the medical device intended for single use?

A.2.24 Is safe decommissioning or disposal of the medical device necessary?

Factors that should be considered include the waste products that are generated during the disposal of the medical device itself. For example, does it contain toxic or hazardous material, or is the material recyclable?

A.2.25 Does installation or use of the medical device require special training?

Factors that should be considered include commissioning and handing over to the end user and whether it is likely/possible that installation can be carried out by people without the necessary skills.

A.2.26 Will new manufacturing processes need to be established or introduced?

The introduction of new manufacturing processes into the manufacturer facilities has to be considered as a potential source of new hazard(s) (e.g., new technology, new scale of production).

A.2.27 Is successful application of the medical device critically dependent on human factors such as the user interface?

Factors that should be considered are user interface design features that can contribute to user error. Features should be designed so that they cannot be easily misused by busy users in an environment where distractions are commonplace, e.g., device control, symbols used, ergonomic features, physical design and layout, hierarchy of operation, menus for software driven devices, visibility of warnings, audibility of alarms, standardized color coding. These considerations include, but are not limited to, the following.

A.2.27.1 Does the medical device have connecting parts or accessories?

Factors that should be considered include the possibility of wrong connections, differentiation, similarity to other products' connections, connection force, feedback on connection integrity, and over- and under-tightening.

A.2.27.2 Does the medical device have a control interface?

Factors that should be considered include spacing, coding, grouping, mapping, modes of feedback, blunders, slips, control differentiation, visibility, direction of activation or change, whether the controls are continuous or discrete, and the reversibility of settings or actions.

A.2.27.3 Does the medical device display information?

Factors that should be considered include visibility in various environments, orientation, populations and perspectives, clarity of the presented information, units, color coding, and the accessibility of critical information.

A.2.27.4 Is the medical device controlled by a menu?

Factors that should be considered include complexity and number of layers, awareness of state, location of settings, navigation method, number of steps per action, sequence clarity and memorization problems, and importance of control function relative to its accessibility.

A.2.28 Is the medical device intended to be mobile or portable?

Factors that should be considered are the necessary grips, handles, wheels, brakes, mechanical stability, and durability.

Annex B
(informative)

Guidance on risk analysis for *in vitro* diagnostic medical devices

B.1 General

This annex provides additional guidance on the risk analysis of *in vitro* diagnostic medical devices, taking into account the particularities and specific aspects of these medical devices. The use of *in vitro* diagnostic medical devices does not create any direct risk to the patient or the person subjected to the examination, as they are not applied in or on the human body. Under certain circumstances, however, indirect risks may result from hazards associated with *in vitro* diagnostic medical devices, leading or contributing to erroneous decisions. In addition, use-related hazards and their associated risks should be considered.

B.2 Identification of hazards

In addition to those aspects mentioned in annex D, the following aspects should be considered in identifying potential hazards for the patient or the person subjected to examination:

— batch inhomogeneity, batch-to-batch inconsistency;

— common interfering factors;

— carry-over effects;

— specimen identification errors;

— stability problems (in storage, in shipping, in use, after first opening of the container);

— problems related to taking, preparation, and stability of specimens;

— inadequate specification of prerequisites;

— inadequate test characteristics.

Potential hazards for the user can arise from radioactive, infectious, toxic, or otherwise hazardous ingredients of reagents and from the packaging design. For instruments, the problem of potential contamination during handling, operation, and maintenance should be considered in addition to the non-specific instrument-related hazards (e.g., energy hazards).

B.3 Risk estimation

In estimating the risk for each hazard, the following aspects should be taken into account:

— extent of reliance on the analytical result (contribution to the medical decision);

— plausibility checks;

— availability and use of controls;

— quality assurance measures/techniques applied in medical laboratories;

— detectability of deficiencies/errors;

— situations of use (e.g., emergency cases);

— professional use/non-professional use;

— method of presentation of information.

Annex C
(informative)

Guidance on risk analysis procedure for toxicological hazards

C.1 General

This annex provides guidance on the application of risk analysis, with respect to toxicological hazards. Toxicological hazards are due to chemical constituents causing biological harm. ISO 10993-1 sets out the general principles for the biological evaluation of materials/medical devices.

Efforts should be made to avoid unnecessary testing using animals. Attention is drawn to ISO 10993-2 on animal welfare requirements, and to relevant national or regional regulations which may indicate that tests should be omitted if the omission can be scientifically justified.

C.2 Estimation of toxicological risks

C.2.1 Factors to be taken into account

The toxicological risk analysis should take account of

— the chemical nature of the materials,

— prior use of the materials, and

— biological safety test data.

The amount of data required and the depth of the investigation will vary with the intended use/intended purpose and are dependent upon the nature and duration of patient contact. Data requirements are usually less stringent for packaging materials, medical devices contacting intact skin, and any component of a medical device that does not come into direct contact with body tissues, infusible liquids, mucous membranes, or compromised skin.

Current knowledge of the material/medical device provided by scientific literature, previous clinical experience, and other relevant data should be reviewed to establish any need for additional data. In some cases, it can become necessary to obtain formulation data, residue data (e.g., from sterilization processes, monomers), biological test data, etc.

C.2.2 Chemical nature of the materials

Information characterizing the chemical identity and biological response of materials is useful in assessing a medical device for its intended use/intended purpose. Some factors that can affect the biocompatibility of the material include:

— the identity, concentration, availability, and toxicity of all constituents (e.g., additives, processing aids, monomers, catalysts, reaction products), and

— the influence of biodegradation and corrosion on the material.

Where reactive or hazardous ingredients have been used in, or can be formed by, the production, processing, storage or degradation of a material, the possibility of exposure to residues should be considered. Information on residue concentration and/or leaching can be necessary. This can take the form of experimental data or information on the chemistry of the materials involved.

Where the necessary data (e.g., complete formulation data) are not available to a manufacturer because of confidentiality, verification should be obtained that an assessment has been carried out of the suitability of the material for use in the proposed application.

C.2.3 Prior use

Available information on previous uses of each material or intended additive and on any adverse reactions encountered should be reviewed. However, the previous use of an ingredient or material does not necessarily assure its suitability in similar applications. Account should be taken of the intended use/intended purpose, the concentration of the ingredients, and current toxicological information.

C.2.4 Biological safety test data

ISO 10993-1 gives guidance on which tests in the ISO 10993 series should be considered for a particular application. The need for testing should be reviewed on a case-by-case basis in the light of existing data, so that unnecessary testing is avoided.

Annex D
(informative)

Examples of possible hazards and contributing factors associated with medical devices

D.1 General

This annex provides a non-exhaustive list of possible hazards together with contributing factors which may be associated with different medical devices. This list may be used to aid in the identification of hazards associated with a particular medical device.

D.2 Energy hazards and contributory factors

These include

— electricity,

— heat,

— mechanical force,

— ionizing radiation,

— non-ionizing radiation,

— moving parts,

— unintended motion,

— suspended masses,

— failure of patient-support device,

— pressure (e.g., vessel rupture),

— acoustic pressure,

— vibration,

— magnetic fields (e.g., MRI).

D.3 Biological hazards and contributory factors

These include

— bio-contamination,

— bio-incompatibility,

— incorrect formulation (chemical composition),

— toxicity,

— allergenicity,

— mutagenicity,

— oncogenicity,

— teratogenicity,

— carcinogenicity,

— re- and/or cross-infection,

— pyrogenicity,

— inability to maintain hygienic safety,

— degradation.

D.4 Environmental hazards and contributory factors

These include

— electromagnetic fields,

— susceptibility to electromagnetic interference,

— emissions of electromagnetic interference,

— inadequate supply of power,

— inadequate supply of coolant,

— storage or operation outside prescribed environmental conditions,

— incompatibility with other devices with which it is intended to be used,

— accidental mechanical damage,

— contamination due to waste products and/or medical device disposal.

D.5 Hazards resulting from incorrect output of energy and substances

These include

— electricity,

— radiation,

— volume,

— pressure,

— supply of medical gases,

— supply of anaesthetic agents.

D.6 Hazards related to the use of the medical device and contributory factors

These include

— inadequate labeling,

— inadequate operating instructions, such as

- inadequate specification of accessories to be used with the medical device,
- inadequate specification of pre-use checks,
- over-complicated operating instructions,
- inadequate specification of service and maintenance,

— use by unskilled/untrained personnel,

— reasonably foreseeable misuse,

— insufficient warning of side effects,

— inadequate warning of hazards likely with re-use of single-use medical devices,

— incorrect measurement and other metrological aspects,

— incompatibility with consumables/accessories/other medical devices,

— sharp edges or points.

D.7 Inappropriate, inadequate, or over-complicated user interface (man/machine communication)

These include

— mistakes and judgment errors,

— lapses and cognitive recall errors,

— slips and blunders (mental or physical),

— violation or abbreviation of instructions, procedures, etc.,

— complex or confusing control system,

— ambiguous or unclear device state,

— ambiguous or unclear presentation of settings, measurements, or other information,

— misrepresentation of results,

— insufficient visibility, audibility, or tactility,

— poor mapping of controls to action, or of displayed information to actual state,

— controversial modes or mappings as compared to existing equipment.

D.8 Hazards arising from functional failure, maintenance, aging, and contributory factors

These include

— erroneous data transfer,

— lack of, or inadequate specification for, maintenance including inadequate specification of post-maintenance functional checks,

— inadequate maintenance,

— lack of adequate determination of the end of life of the medical device,

— loss of electrical/mechanical integrity,

— inadequate packaging (contamination and/or deterioration of the medical device),

— re-use and/or improper re-use,

— deterioration in function (e.g., gradual occlusion of fluid/gas path, or change in resistance to flow, electrical conductivity) as a result of repeated use.

Annex E
(informative)

Risk concepts applied to medical devices

E.1 Risk estimation

Various methods can be used to estimate risk. While this International Standard does not require that a particular method be used, it does require that risk estimation is carried out (see 4.4). Quantitative risk estimation is possible when suitable data are available. Methods for quantitative risk estimation could merely include the adaptation of a qualitative method, or an alternative approach might be appropriate.

A risk chart such as Figure E.1 can be used as part of a qualitative method to define risk. Figure E.1 is an example of a risk chart and is included only to show the method. This does not imply that it has general application to medical devices. If a risk chart approach is used for estimating risk, the particular risk chart and the interpretation used should be justified for that application.

The concept of risk is the combination of the following two components:

— the probability of occurrence of harm, that is, how often the harm may occur;

— the consequences of that harm, that is, how severe it might be.

Risk estimation should examine the initiating events or circumstances, the sequence of events that are of concern, any mitigating features, and the nature and frequency of the possible deleterious consequences of the identified hazards. Risk should be expressed in terms that facilitate risk control decision making. In order to analyze risks, their components, i.e., probability and severity, should be analyzed separately.

E.2 Probability

E.2.1 Probability estimation

In appropriate situations where sufficient data are available, a quantitative categorization of probability levels is to be preferred. If this is not possible, the manufacturer should give a qualitative description. A qualitatively good description is preferable to quantitative inaccuracy. For a qualitative categorization of probability levels, the manufacturer can use descriptors appropriate for the medical device. The concept is in reality a continuum, however in practice a number of discrete levels can be used. In this case, the manufacturer decides how many categories are needed and how they are to be defined. The levels can be descriptive (e.g., incredible, improbable, remote, occasional, probable, frequent) or symbolic (P1, P2, etc.).

Probability estimation examines the initiating events or circumstances and the sequence of events that are of concern. This includes answering the following questions.

— Does the hazard occur in the absence of a failure?

— Does the hazard occur in a failure mode?

— Does the hazard occur only in a multiple-fault condition?

The probability of each undesired event occurring is identified at the hazard-identification stage. Three approaches are commonly employed to estimate probabilities, as follows:

— use of relevant historical data,

— prediction of probabilities using analytical or simulation techniques,

— use of expert judgment.

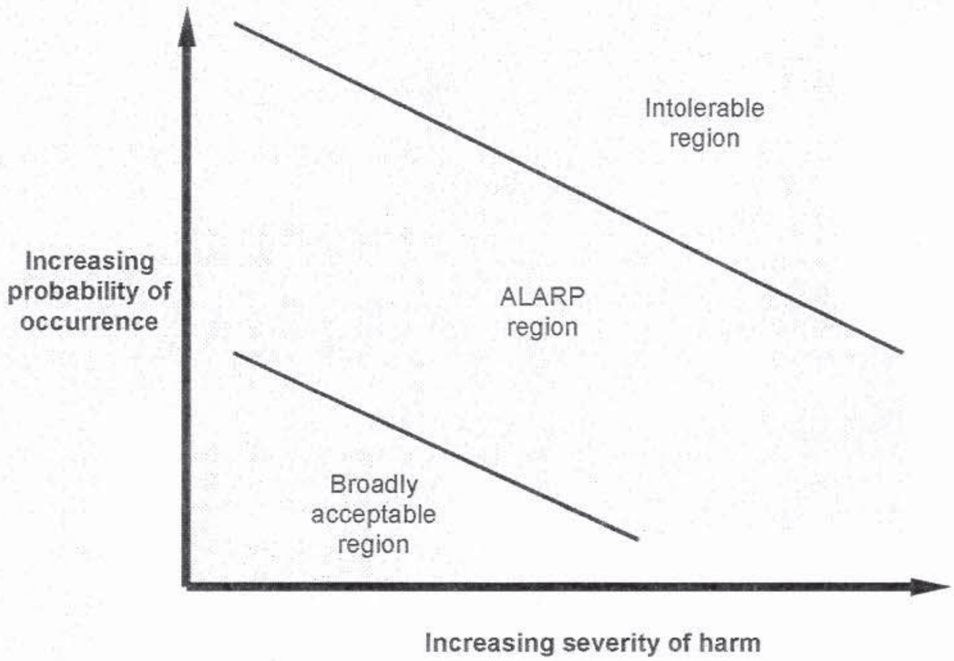

Figure E.1—Example of a three-region risk chart

All these approaches can be used individually or jointly. The first two approaches are complementary; each has strength where the other has weaknesses. Wherever possible, both should be used. In this way, they can be used as independent checks on each other, and this might serve to increase confidence in the results. When these cannot be used or are not sufficient, it might be necessary to rely on expert judgment.

Some hazards occur because of systematic rather than random failures. For example, hazards derived from software failures are due to systematic failures. For a discussion on how to address systematic failures, see E.4.3.

E.2.2 Severity levels

For a qualitative categorization of the levels of severity, the manufacturer should use descriptors appropriate for the medical device. The concept is in reality a continuum, however in practice a number of discrete levels can be used. In this case, the manufacturer decides how many categories are needed and how they are to be defined. The levels may be descriptive (e.g., negligible, marginal, critical, serious, catastrophic) or symbolic (S1, S2, etc.).

These levels will need to be customized by the manufacturer for a particular medical device considering both short-term and long-term effects.

E.3 Risk acceptability

E.3.1 General

This International Standard does not specify acceptable risk. Methods of determining acceptable risk include the following:

— using applicable standards that specify requirements which, if implemented, will indicate achievement of acceptability concerning particular kinds of medical devices or particular risks;

— following appropriate guidance, for example, that obtained by using the single-fault philosophy (for details, see 9.10 of IEC/TR 60513:1994);

— comparing levels of risk evident from medical devices already in use.

Risk should only be accepted in a particular situation if it is outweighed by benefits.

Risks can be categorized into the following three regions:

— broadly acceptable region;

— ALARP (As Low As Reasonably Practicable) region;

— intolerable region.

A three-region concept of risk is illustrated in Figure E.1. These regions will need to be customized for a particular medical device.

Examples of the use of numerical probability and severity estimates can be found in some of the standards listed in the bibliography. Users of this International Standard are urged to define probability and severity categories applicable to their own particular application.

E.3.2 Broadly acceptable region

In some cases, a risk is so low that it is negligible in comparison with other risks and in view of the benefit of using the medical device. In such cases, the risk is acceptable, and risk control need not be actively pursued.

E.3.3 ALARP region

It might be thought that any risk associated with a medical device would be acceptable if the patient's prognosis were improved. This cannot be used as a rationale for the acceptance of unnecessary risk. Any risk should be reduced to the lowest level practicable, bearing in mind the benefits of accepting the risk and the practicability of further reduction.

Practicability refers to the ability of a manufacturer to reduce the risk. Practicability has two components:

a) technical practicability, and

b) economic practicability.

Technical practicability refers to the ability to reduce the risk regardless of cost. Economic practicability refers to the ability to reduce the risk without making the provision of the medical device an unsound economic proposition. Cost and availability implications are considered in deciding what is practicable to the extent that these impact upon the preservation, promotion, or improvement of human health.

Major risks should normally be reduced even at considerable cost. Near the broadly acceptable region, a balance between risk and benefit may suffice.

E.3.4 Intolerable region

Some risks, if they cannot be reduced, may always be judged intolerable.

E.3.5 Risk-acceptability decisions

There is an important distinction to be made between risks that are so low that there is no need to consider them and risks which are greater than that but which we are prepared to live with because of the associated benefits and the impracticality of reducing the risks. When a hazard has been identified and the risk estimated, the first question to be asked is whether the risk is already so low that there is no need to consider it and therefore no need to progress to risk reduction. This decision is made once for each hazard.

If the decision at the first stage is that the risk is not so low that there is no need to consider it, the next stage is to progress to risk reduction. Risk reduction might or might not be practicable, but it should be considered. The possible outcomes of this second stage are as follows:

— that one or more risk-reduction measures bring the risk down to a level where it is not necessary to consider it further; or

— that, whether or not some risk reduction is possible, reducing the risk down to the "no need to consider it" level is not practicable.

In the latter case, the risk should be reduced to a level as low as reasonably practicable (ALARP), and then the risk and benefit should be compared. If the risk is outweighed by the benefit, then the risk may be accepted. If the risk <u>is not</u> outweighed by the benefit, then it is unacceptable, and the design should be abandoned.

Finally, once all risks have been found to be acceptable, the overall residual risk is evaluated to assure that the risk/benefit balance is still maintained.

Thus, there are three decision points in the process, where different questions are asked about the acceptability of risks:

a) Whether the risk is so low that there is no need to consider it?

b) Whether there is no longer any reason to consider the risk, or the risk is as low as is reasonably practicable and outweighed by the benefit?

c) Whether the overall balance of all the risks with all the benefits is acceptable?

E.4 Cause of failure

E.4.1 Failure types

A hazardous situation can result from the failure of a system. There are two possible types of failure:

— random failures, and

— systematic failures.

E.4.2 Random failure

For many events, a statistical probability of failure can be assigned (e.g., the probability of failure of an assembly is often estimated from the failure probabilities of the components which make up the assembly). In this case, a numerical value can be given for the probability of failure. An essential presumption is that the failures are random in nature. Hardware is assumed to fail either in a random or in a systematic manner. Software is assumed to fail in a systematic manner.

E.4.3 Systematic failure

Systematic failures are due to errors (including errors of commission and omission) in any activity which, under some particular combination of inputs or environmental conditions, will permit a failure.

The error leading to systematic failures can occur in both hardware and software and can be introduced at any time during a medical device's development, manufacture, or maintenance. Examples of a systematic failure are as follows:

a) An incorrectly rated fuse fails to prevent a hazardous situation. The fuse rating might have been incorrectly specified, incorrectly fitted during manufacture, or incorrectly replaced during repair.

b) The use of incorrect material in a joint replacement results in excessive wear and premature failure of a hip implant. The incorrect material may have been incorrectly specified or incorrectly used during manufacture (e.g., the incorrect material is ordered from the supplier).

c) A software database does not provide for the condition of full database. If the database is full, it is not clear what the software will do. A possible consequence is that the system will delete existing records to make room for new ones.

The accurate estimation of systematic failure rates is difficult. This occurs primarily for the two following reasons:

a) Systematic failure rates are laborious and expensive to measure. Achieving a reasonable level of confidence in the result will not be possible without a long history of measuring failure rates.

b) Consensus does not exist for a method of estimating systematic failure rates quantitatively.

In cases where an appropriate level of confidence cannot be established for the estimation of systematic failures, the risk should be managed based on the severity of the harm resulting from the hazard. Initially, the risk estimation for systematic faults should be based on the presumption that systematic failure will occur at an unacceptable rate.

There is a relationship between the quality of the development processes used and the possibility of a systematic fault being introduced or remaining undetected. It is often appropriate to determine the required quality of the development process by taking account of the severity of the consequence of the systematic faults and the effect of external risk-control measures. The worse the consequence and the less the effect of external risk-control measures, the higher the required quality of the development process.

Annex F
(informative)

Information on risk analysis techniques

F.1 General

This annex provides guidance on some available techniques for probabilistic safety analysis that can be used under 4.3. These techniques are complementary and it might be necessary to use more than one of them. The basic principle is that the possible consequences of a postulated event are analyzed step by step. For further details, see also IEC 60300-3-9.

F.2 Failure Mode and Effect Analysis (FMEA)

FMEA is primarily a qualitative technique by which the consequences of an individual component fault mode are systematically identified and evaluated. It is an inductive technique using the question "What happens to the output if . . .?" Components are analyzed one at a time, thus generally looking at a single-fault condition. This is done in a "bottom-up" mode, i.e., following the process to the next higher functional system level.

FMEA can be extended to incorporate an investigation of the degree of severity of the consequences, their respective probabilities of occurrence and their detectability, and can become a so-called Failure Mode Effect and Criticality Analysis (FMECA). In order to perform such an analysis, the construction of the medical device should be known in some detail.

FMEA can also be a useful technique to deal with human error. It can also be used to identify hazards and thus provide valuable input to a Fault Tree Analysis (FTA).

Disadvantages of this technique can arise from difficulties in dealing with redundancies and the incorporation of repair or preventive maintenance actions, as well as its restriction on single-fault conditions.

See IEC 60812 for more information on the procedures for failure mode and effects analysis.

F.3 Fault Tree Analysis (FTA)

FTA is primarily a means of analyzing hazards identified by other techniques and starts from a postulated undesired consequence, also called a "top event." In a deductive manner, starting with the top event, the possible causes or fault modes of the next lower functional system level causing the undesired consequence are identified. Following stepwise identification of undesirable system operation to successively lower system levels will lead to the desired system level, which is usually the component fault mode. This will reveal the sequences most likely to lead to the postulated consequence. It has therefore proved to be useful for forensic purposes.

The results are represented pictorially in the form of a tree of fault modes. At each level in the tree, combinations of fault modes are described with logical operators (AND, OR, etc.). The fault modes identified in the tree may be events that are associated with hardware failures, human errors, or any other pertinent event which leads to the undesired event. They are not limited to the single-fault condition.

FTA allows a systematic approach which, at the same time, is sufficiently flexible to allow analysis of a variety of factors, including human interactions. FTA is primarily used in risk analysis as a tool to provide an estimate of failure probabilities. The pictorial representation leads to an easy understanding of the system behavior and the factors included, but, as the trees become large, processing of fault trees may require computer systems. This feature makes the verification of the fault tree difficult.

See IEC 61025 for more information on the procedures for fault tree analysis.

F.4 Hazard and Operability Study (HAZOP)

HAZOP is similar to an FMEA. HAZOP is based on a theory that assumes accidents are caused by deviations from the design or operating intentions. It is a systematic technique for identifying hazards and operability problems. It was originally developed for use in the chemical process industry. While the use of HAZOP studies in the chemical industry focuses on deviations from design intent, there are alternative applications for a medical device developer. A HAZOP can be applied to the operation of the medical device (e.g., to the existing methods/processes used for the diagnosis, treatment, or alleviation of disease as the "design intent"), or to a process used in the manufacture or maintenance of the medical device (e.g., sterilization) that may have significant impact on the function of the medical device. Two particular features of a HAZOP are as follows:

a) it uses a team of people with expertise covering the design of the medical device and its application; and

b) guide words (NONE, PART OF, etc.) are used to help identify deviations from normal use.

The objectives of the technique are

— to produce a full description of the medical device and how it is intended to be used,

— to review systematically every part of the intended use/intended purpose to discover how deviations from the normal operating conditions and the intended design can occur,

— to identify the consequences of such deviations and to decide whether these consequences can lead to hazards or operability problems.

When applied to the processes used to manufacture a medical device, the last objective is particularly useful in those cases where the medical device characteristics depend upon the manufacturing process.

Annex G
(informative)

Other standards that contain information related to the elements of risk management described in this International Standard

Table G.1—Quality management elements that may be related to the elements of risk management

Overview of the risk management process		Subclauses of ISO 13485:1996 [a] 4.1	4.2 (see note 1)	4.3	4.4	4.5	4.6	4.7	4.8	4.9	4.10	4.11	4.12	4.13	4.14	4.15	4.16 (see note 2)	4.17	4.18	4.19	4.20
General requirements																					
Risk analysis	Scope definition																				
	Hazard identification																				
	Risk estimation																				
Risk evaluation																					
Risk control	Analysis of options																				
	Decision making																				
	Implementation																				
Post-production information																					

NOTE 1—Risk management can be part of a quality management system.

NOTE 2—The risk management file can include quality records.

[a] Shaded areas indicate the parts of the risk management process which might be related to this International Standard.

Table G.2—Other International Standards that may be related to the elements of risk management

Overview of the risk management process		Applicable standards[a]										
		ISO 9001	ISO 9000-3	ISO 10993-1	ISO 13485	ISO 14969	IEC 60300-3-9	IEC/TR 60513	IEC 60601-1-4	IEC 60812	IEC 61025	EN 12442-1
Risk analysis	Scope definition											
	Hazard identification											
	Risk estimation											
Risk evaluation												
Risk control	Analysis of options											
	Decision making											
	Implementation											
Post-production information												

[a] Shaded areas indicate the parts of the risk management process which might be related to these International Standards.

Bibliography

[1] ISO/IEC Guide 2:1996, *Standardization and related activities—General vocabulary.*

[2] ISO/IEC Guide 51:1999, *Safety aspects—Guidelines for the inclusion in standards.*

[3] ISO 8402:1994[1], *Quality management and quality assurance—Vocabulary.*

[4] ISO 9000-3:1991, *Quality management and quality assurance standards—Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software.*

[5] ISO 9001:—[2], *Quality management systems—Requirements.*

[6] ISO 10993-1, *Biological evaluation of medical devices—Part 1: Evaluation and testing.*

[7] ISO 10993-2, *Biological evaluation of medical devices—Part 2: Animal welfare requirements.*

[8] ISO 10993-17, *Biological evaluation of medical devices—Part 17: Establishment of allowable limits for leachable substances using health-based risk assessment.*

[9] ISO 13485, *Quality systems—Medical devices—Particular requirements for the application of ISO 9001.*

[10] ISO 13488, *Quality systems—Medical devices—Particular requirements for the application of ISO 9002.*

[11] ISO 14969, *Quality systems—Medical devices—Guidance on the application of ISO 13485 and ISO 13488.*

[12] ISO 15189, *Quality management in the medical laboratory.*

[13] IEC 60300-3-9, *Dependability management—Part 3: Application guide—Section 9: Risk analysis of technological systems.*

[14] IEC/TR 60513, *Fundamental aspects of safety standards for medical electrical equipment.*

[15] IEC 60601-1:1988, *Medical electrical equipment—Part 1: General requirements for safety.*

[16] IEC 60601-1-4, *Medical electrical equipment—Part 1: General requirements for safety—4: Collateral standard: Programmable electrical medical systems.*

[17] IEC 60812, *Analysis techniques for system reliability—Procedures for failure mode and effects analysis (FMEA).*

[18] IEC 61025, *Fault tree analysis (FTA).*

[19] IEC 61882, *Guide for hazard and operability studies (HAZOP studies).*

[20] EN 12442-1, *Animal tissues and their derivatives utilized in the manufacture of medical devices—Part 1: Analysis and management of risk.*

[21] 90/285/EEC, *Council Directive of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (90/385/EEC)* as amended by *Council Directive 93/42/EEC of 14 June 1993 concerning medical devices* and *Council Directive 93/68/EEC of 22 July 1993.*

[22] 93/42/EEC, *Council Directive 93/42/EEC of 14 June 1993 concerning medical devices* as amended by *Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices.*

[23] 98/79/EC, *Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices.*

---

1) This is under revision and will be reissued as ISO 9000:2000.

2) To be published. (Revision of ISO 9001:1994, ISO 9002:1994, and ISO 9003:1994.)